UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

ANDERSON's residence, 2424 W. Wells Street, Apt 114, Milwaukee Wisconsin 53233 (SUBJECT PREMISES), ANDERSON's vehicle a white GMC Yukon license plate ALU6909 (SUBJECT VEHICLE), and ANDERSON's person (DOB XX/XX/1969)

Case No. 24 MJ 11

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Please see Attachment A.

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252(a)(2)(A)	Production of Child Pornography
18 U.S.C. § 1591(a)(1)(b)(1)	Sex Trafficking of a Minor
18 U.S.C. § 2251	Sexual Exploitation of a Child
18 U.S.C. § 2252(a)(2)	Receipt of Child Pornography

The application is based on these facts:

Please see Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Sarah Dettmering, Special Agent, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 01/08/2024

Judge's signature

City and state: Milwaukee, WI

Honorable William E. Duffin, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Sarah Dettmering, being first duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent of the Federal Bureau of Investigation (FBI) since January 2018 and am currently assigned to the Milwaukee Division as a member of the Milwaukee Child Exploitation and Human Trafficking Task Force. My duties include investigating criminal violations relating to child sexual exploitation and child pornography. While employed by the FBI, I have investigated federal criminal violations related to child exploitation and child pornography. I have received training from the FBI specific to investigating child pornography and child exploitation crimes and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media. As a result of my training, experience, and discussions with other law enforcement officers assigned to investigate child pornography and child exploitation, I am familiar with methods by which electronic devices are used as the means for receiving, transmitting, possessing, and distributing images and videos depicting minors engaged in sexually explicit conduct. I have also received training and gained experience in interview and interrogation techniques with enhanced training specific to cybercrimes, social media search warrants, residential search warrants, interviews and interrogations of subjects of criminal investigations, electronic device identification and forensic review.

2. The facts contained in this affidavit are known to me through my personal knowledge, training, and experience, and through information provided to me by other law

enforcement officers, who have provided information to me during the course of their official duties and whom I consider truthful and reliable.

3. Based upon the information described below, I submit that probable cause exists to believe that Daniel ANDERSON, date of birth XX/XX/1969, has committed the crime of production of child pornography in violation of Title 18, United States Code, § 2252(a)(2)(A); sex trafficking of a minor in violation of Title 18, United States Code, § 1591(a)(1)(b)(1); sexual exploitation of a child in violation of Title 18, United States Code, § 2251; and receipt of child pornography in violation of Title 18, United States Code, § 2252(a)(2). I further submit that evidence relating to this crime, more particularly described in Attachment B, can be found at ANDERSON's residence, 2424 W. Wells Street, Apt 114, Milwaukee Wisconsin 53233 (SUBJECT PREMISES), on ANDERSON's person, or in ANDERSON's vehicle a white GMC Yukon license plate ALU6909 (SUBJECT VEHICLE), more particularly described in Attachment A. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

DEFINITIONS

4. The following definitions apply to the Affidavit and Attachment B to this Affidavit:

a. "Child Pornography" is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

b. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

c. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

e. "Visual depictions" include undeveloped film and videotape, and data stored on a computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

ELECTRONIC STORAGE DEVICES AND FORENSIC ANALYSIS

5. I am aware through training, experience, and consulting with other law enforcement agents/analysts with specialized knowledge and training in computers, networks, and Internet communications that to properly retrieve and analyze electronically stored (computer) data, and to

ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the electronic storage devices. To ensure such accuracy and completeness, it may also be necessary to analyze not only the electronic storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the device computer and software. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the proposed search location, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive, other storage media, within a hand-held electronic device such as a cellular telephone or a tablet device (e.g., an iPad device). Some of this electronic information, as explained below, might take a form that becomes meaningful only upon forensic analysis.

6. Based on my knowledge, training, and experience, I know that computer and other electronic device hardware, peripheral devices, software, documentation, and passwords may be important to a criminal investigation in three distinct and important respects:

a. The objects themselves may be instrumentalities used to commit the crime.

b. The objects may have been used to collect and store information about crimes (in the form of electronic data).

c. The objects may be contraband or fruits of the crime.

7. I submit that if a computer or other electronic storage device is found on the premises, there is probable cause to believe those records will be stored in that electronic storage device, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that electronic storage device files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person deletes a file on an electronic storage device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. It follows that deleted files, or remnants of deleted files, may reside in free space or slack spaceCthat is, in space on the storage medium that is not currently being used by an active file for long periods of time before they are overwritten. In addition, if the electronic storage device uses an operating system (in the case, for example, of a computer, cellular telephone, or tablet device) the device may also contain a record of deleted data in a swap or recovery file.

b. Wholly apart from user-generated files, electronic storage device storage media in particular, computers' internal hard drives, contain electronic evidence of how the device was used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, and file system data structures. Electronic storage device users typically do not erase or delete this evidence because special software is typically required for that task. However, it is technically possible to delete this information.

c. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or cache. The browser often maintains a fixed

amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

8. As further described in Attachment B, this application seeks permission to locate not only electronic storage device files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how electronic storage devices were used, the purpose of their use, who used them, and when.

9. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), electronic storage device storage media can contain other forms of electronic evidence as described below:

a. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the electronic storage device was in use. Electronic storage device file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within an electronic storage device and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion.

In my training and experience, information stored within an electronic storage device (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the electronic storage device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the electronic storage device was remotely accessed, thus inculpating or exculpating the electronic storage device owner. Further, electronic storage device activity can indicate how and when the electronic storage device was accessed or used. For example, as described herein, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within an electronic storage device may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or cellular telephone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera). The geographic and timeline information described herein may either inculpate or exculpate the electronic storage device user. Last,

information stored within an electronic storage device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information within the electronic storage device may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the electronic storage device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on an electronic storage device is relevant to the investigation may depend on other information stored on the electronic storage device and the application of knowledge about how an electronic storage device works. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

d. Further, in finding evidence of how an electronic storage device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, I know from training and experience that it is possible that malicious software can be installed on a computer, often without the computer user's knowledge, that can allow the computer to be used by others, sometimes without the knowledge of the computer owner.

10. Based upon my knowledge, training and experience, and after having consulted with FBI computer forensic personnel, I know that a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a

controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some electronic storage device equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how an electronic storage device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.

b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. Technical requirements. Electronic storage devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of electronic storage device hardware and software available makes it difficult to know before a search what tools or knowledge will be required to

analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

11. In light of these concerns, I hereby request the Court's permission to seize the electronic storage devices, associated storage media, and associated peripherals that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the hardware, media, or peripherals on-site for this evidence.

12. I know that when an individual uses a computer to commit crimes involving child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic storage device is an instrumentality of the crime because it is used as a means of committing the criminal offense. From my training and experience, I believe that an electronic storage device used to commit a crime of this type may contain data that is evidence of how the electronic storage device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

BIOMETRIC ACCESS TO DEVICES

13. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

14. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

15. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face.

Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

16. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

17. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

18. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

19. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

20. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, I request authority for law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of ANDERSON, to the fingerprint scanner of the devices found on ANDERSON or at the SUBJECT PREMISES or in the SUBJECT VEHICLE; (2) hold the devices found on ANDERSON, in the SUBJECT VEHICLE or at the SUBJECT PREMISES in front of ANDERSON's face to activate the facial recognition feature; and/or (3) hold the devices found on ANDERSON, in the SUBJECT VEHICLE or at the SUBJECT PREMISES in front of ANDERSON's face and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

21. On or about September 6, 2023, FBI Memphis received information from the Lauderdale County Sheriff's Office (LCSO) regarding allegations that Child Sexual Abuse Material, also known as Child Pornography, hereinafter referred to as CSAM, of a twelve-year-old-girl, hereinafter Victim 1, was produced and distributed by Victim 1's mother, hereinafter C.E.

22. On or about July 14, 2023, a forensic interview was conducted of Victim 1 and notes were taken by the witnessing law enforcement officer from LCSO. Based upon the notes of the officer which I have reviewed, Victim 1 made several disclosures, which included:

a. When Victim 1 was 10 to 11 years old, Victim 1 lived with C.E. in Milwaukee, Wisconsin. During that time Victim 1 was introduced to an adult male who was later identified by law enforcement to be Daniel ANDERSON[1].

b. C.E. asked Victim 1 if C.E. could take pictures of Victim 1's body. Victim 1 saw messages on C.E.'s phone between C.E. and ANDERSON which showed that ANDERSON was asking C.E. to take the pictures of Victim 1. Victim 1 recalled one message stated, "if you get her to do it, I'll give you this amount of money."

c. The first time C.E. took pictures of Victim 1, they were in the apartment in Milwaukee, Wisconsin. C.E. told Victim 1 to pull down Victim 1's pants, lay down on the couch, and open Victim 1's legs. C.E. then took pictures of Victim 1's vagina, C.E. instructed Victim 1

[1] Victim 1 originally identified the male as "Dan Henderson," but through the investigation of law enforcement officers and further interviews of C.E. it was determined that the individual's name was actually "Daniel ANDERSON." "Dan Henderson's" driver's license image was shown to Victim 1, and Victim 1 said that was not the man that Victim 1 was referring to. After a review of C.E.'s cell phone, ANDERSON's CashApp was observed, as the account sent C.E. money. C.E. also used the name "Danny ANDERSON" during her interviews with law enforcement.

to "open her vagina" for the picture. Victim 1 then observed C.E.'s phone, which showed that C.E. sent the pictures to ANDERSON.

d. Victim 1 took the pictures that C.E. requested because Victim 1 was afraid of C.E.'s threats to "whoop" Victim 1. Victim 1 explained that "whoop" meant getting punched.

e. Victim 1 saw on C.E.'s phone that ANDERSON sent C.E. $600 on CashApp after C.E. sent ANDERSON the nude picture of Victim 1.

f. Victim 1 disclosed another time C.E. took pictures of Victim 1 while Victim 1 was in the shower, nude.

g. Victim 1 disclosed that on one occasion, C.E. took Victim 1 to ANDERSON's apartment in Milwaukee, Wisconsin. Victim 1 recalled that ANDERSON's apartment number was 114 and it was on "Wells"[2] Street. While at the apartment, Victim 1 was brought to a bedroom with a man named "Brian." C.E. told Victim 1 to pull down Victim 1's clothes, open Victim 1's legs, and lay down in bed. C.E. and Brian got into bed with Victim 1. ANDERSON was there and "made it dark in the room." C.E. covered the top of Victim 1's body and Victim 1's face with a white hospital blanket. Victim 1 then felt a rough finger, which Victim 1 believed to be Brian's touching around her privates while C.E. and Brian "hunched[3]." When C.E. told Victim 1 that they were done, ANDERSON took C.E. and Victim 1 out to eat and ANDERSON gave C.E. money.

---

[2] The report written by the reviewing officer stated that Victim 1 said "Walls" Street, however after I listened to the recording of the interview Victim 1 appears to state "Wells" Street.

[3] Victim 1 did not clarify or explain what she meant by "hunched," but based on my contextual review, I believe this to mean that C.E. and "Brian" were also engaged in sexual activity while "Brian" was simultaneously touching around Victim 1's private parts.

h. Victim 1 recalled seeing pictures of other girls around Victim 1's age on C.E.'s phone, which were sent to C.E. by ANDERSON.

23. On or about October 23, 2023, C.E. agreed to participate in an interview with an FBI Task Force Officer. I have reviewed the report from this interview, and C.E. made statements which included:

a. C.E. took nude images of Victim 1 and sent them to "Dan" in Milwaukee. C.E. identified "Dan" as Daniel ANDERSON. ANDERSON told C.E. to take the sexually explicit pictures of C.E.'s minor daughter and send them to ANDERSON in exchange for money.

b. C.E. described ANDERSON as in his 50's, brown skin, tall and drives a new model white truck. C.E. had the phone number 757-334-0611 for ANDERSON.

c. C.E. showed the TFO C.E.'s CashApp account which showed a payment from ANDERSON to C.E. on or about June 24, 2023 for $40. This payment was for a nude image of C.E.'s minor daughter, Victim 1. The account name that sent C.E. the money was "Danny ANDERSON" and the image associated with the account bore a strong resemblance to the driver's license image of ANDERSON.

d. ANDERSON would tell C.E. to take nude images of Victim 1, and would threaten C.E. if C.E. did not. C.E. did not explain the nature of the threats. ANDERSON sent C.E. images of other minor girls to show C.E. what he expected for pictures of Victim 1. C.E. then took the nude pictures of Victim 1 and sent them to ANDERSON. ANDERSON paid C.E. $60-$80 for the images. ANDERSON had naked images of other girls on ANDERSON's phone.

e. ANDERSON brought girls Victim 1's age, 11 to 12 years old, to the Potawatomi Casino in Milwaukee to have sex with men. C.E. witnessed ANDERSON bringing the girls to the casino and had conversations with ANDERSON about it.

24. On or about October 30, 2023, C.E. was again interviewed by the same FBI TFO. During this interview, C.E. identified ANDERSON from ANDERSON's driver's license picture as well as ANDERSON's Wisconsin Sex Offender Registry picture as the individual who paid C.E. for naked pictures of Victim 1. C.E. was shown pictures of the apartment building in which the SUBJECT PREMISES is located and C.E. identified that as the building where ANDERSON lived. C.E. believed the apartment number was 113 or 114.

25. C.E. also placed a consensually recorded call to ANDERSON at phone number 757-334-0611, ANDERSON answered and stated that ANDERSON recently had a "hotel party." After the call C.E. told the TFO that a "hotel party" was where minor girls were present to have sex with adult men.

26. On or about November 3, 2023, C.E. was again interviewed by the same FBI TFO. I have reviewed the report written by the TFO, which stated that C.E. made statements including:

a. ANDERSON set up "dates" for C.E. on two occasions. C.E. went to ANDERSON's apartment where C.E. had sex with a man for $75. ANDERSON told C.E. to bring Victim 1 for the date. Victim 1 was in the bed during C.E.'s second date, while C.E. had sex with the man.

b. ANDERSON set up dates for older white men to have sex with underage black girls. C.E. witnessed ANDERSON let men into ANDERSON's apartment, then shortly after,

a young girl would show up. On one occasion C.E. traveled with ANDERSON to pick up a fourteen-year-old girl.

27. On or about November 10, 2023, C.E. was again interviewed by the same FBI TFO. I have reviewed the report written by the TFO, and listened to the interview recording, C.E. made statements including:

a. C.E. accompanied ANDERSON to rent rooms at the casino and watched young girls be brought inside. ANDERSON made C.E. sit by a slot machine so C.E. did not go with ANDERSON and the girls to the room. This happened approximately 15 times in or around January and February of 2023.

b. ANDERSON is at the casino every weekend. A casino worker helps ANDERSON. C.E. stated in the interview that the worker was "in on it" and was receiving money for helping ANDERSON. C.E. did not specify the nature of the help the casino worker provided.

c. C.E. went with ANDERSON in ANDERSON's vehicle to pick up minor girls and watched ANDERSON bring the girls to his apartment. While in ANDERSON's vehicle, C.E. saw older white men arrive and be admitted to the apartment by ANDERSON.

d. C.E. stated in the interview that on one occasion C.E. brought Victim 1 to ANDERSON's apartment, and ANDERSON "did touch my baby." C.E. disclosed that ANDERSON had Victim 1 get naked and asked C.E. to have sex with ANDERSON while Victim 1's clothes were off. ANDERSON touched Victim 1's breasts while C.E. and ANDERSON were having sex.

e. C.E. saw nude images of Victim 1 on ANDERSON's phone, which was an iPhone. C.E. sent nude images of Victim 1 to ANDERSON after ANDERSON asked for the nude

images. C.E. saw images of other minor girls as well on the phone. C.E. did not specifically state that these images were sexually explicit, however, C.E. was asked about the pictures of other minor girls immediately following being asked about the explicit images of Victim 1 which made it seem as though these images were also sexually explicit.

f. ANDERSON drove a white Yukon style truck, which matches the description of the SUBJECT VEHICLE.

g. Clients paid ANDERSON for sex with minors via the mobile application CashApp, ANDERSON told C.E. that the clients paid him via CashApp.

28. In the past C.E. has been on the phone with ANDERSON and ANDERSON would say he had to go because it had to set up a date. ANDERSON would say he had to go down to Potawatomi to get a room.

29. On or about November 9, 2023, an administrative subpoena was issued to Verizon Wireless for phone number 757-334-0611. The subscriber information listed the user as "Debbie Hughes" in Portsmouth Virginia and the device as an iPhone 13. C.E. described ANDERSON's phone as an iPhone. I know from my training and experience that subjects engaged in criminal activity will sometimes use a false name in order to prevent records from identifying them. Therefore, "Debbie Hughes" is likely a false name as the number was known to be used by ANDERSON subsequent to the subpoena.

30. On or about July 5, 2023, ANDERSON was contacted by a Milwaukee County Sheriff's Deputy during a traffic accident which ANDERSON was a part of and provided 757-334-0611 as his phone number. ANDERSON was driving the SUBJECT VEHICLE, which was the style described by C.E. At that time ANDERSON did provide a different address than the

SUBJECT PREMISES to the responding deputy, he gave the address of 956 N 27th Street, Milwaukee.

31. Employment records for ANDERSON showed that ANDERSON worked for Prolec-GE Waukesha (GE) and Western Building Products in Milwaukee (WBP). On or about January 2, 2024, ANDERSON was observed by FBI Agents at GE, and entered the SUBJECT VEHICLE. ANDERSON then drove the SUBJECT VEHICLE to WBP. Later that day ANDERSON was observed driving the SUBJECT VEHICLE and entered the parking garage at the SUBJECT PREMISES.

32. On or about January 3, 2024, the SUBJECT VEHICLE was observed parked in the garage attached to the apartment complex in which the SUBJECT PREMISES is located.

33. ANDERSON's profile on Wisconsin's Sex Offender Registry listed 2424 W Wells Street, Apt 114, Milwaukee, Wisconsin as ANDERSON's address but it was last verified in or about May 2023.

34. Based upon the interview with Victim 1 and C.E., ANDERSON had C.E. bring Victim 1 to the SUBJECT PREMISES where Victim 1 was sexually assaulted while C.E. engaged in sexual activity with an adult man. Based upon the interviews with C.E., ANDERSON used his apartment in order to arrange for older men to have sex with underage girls, and ANDERSON resided at this address when ANDERSON requested and received nude images of Victim 1.

35. Based upon the provided information there is probable cause to believe that ANDERSON violated federal law while residing at the SUBJECT PREMISES, ANDERSON still resides at the SUBJECT PREMISES, ANDERSON used the SUBJECT VEHICLE is furtherance of criminal activity, and ANDERSON used a cell phone in furtherance of criminal activity.

Therefore, there is probable cause that evidence of criminal activity will be at the SUBJECT PREMISES, in the SUBJECT VEHICLE and on the person of ANDERSON.

36. On or about January 4, 2024, a Special Agent with the FBI made contact with the apartment manager, hereinafter N.M. for the SUBJECT PREMISES. N.M provided the lease agreement for ANDERSON which stated that ANDERSON rented apartment 114. The "Parking Addendum" to the lease agreement stated that ANDERSON's vehicle was the SUBJECT VEHICLE. N.M. stated that ANDERSON was a current resident of the SUBJECT PREMISES.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

37. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following: Computers, cellular telephones, and other electronic storage devices (collectively electronic storage devices) have dramatically changed the way in which individuals interested in child pornography interact with each other. Electronic storage devices basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

38. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a device by simply connecting the camera to the electronic storage device. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store terabytes of

data, which provides enough space to store thousands of high-resolution photographs. Video recorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the video recorder to a computer. Many electronic storage devices (e.g., computers, cellular telephones, and tablets), have cameras built into the device which allows users to create and store still and video images on the device. Moreover, if the device has internet connectivity, users can distribute still and video images from the device.

39. Internet-enabled electronic storage devices can connect to other internet-enabled devices the world over. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to an internet-enabled electronic storage device. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, electronic storage devices are the preferred method of distribution and receipt of child pornographic materials.

40. Electronic storage devices are the ideal repository for child pornography. The amount of information that an electronic storage device can hold has grown exponentially over the last decade. Electronic storage devices can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged

into a port on a computer or other electronic storage device. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Many electronic storage devices can easily be concealed and carried on an individual's person.

41. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

42. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Google, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any internet-enabled electronic storage device. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's electronic storage device in most cases.

43. As is the case with most digital technology, communications by way of electronic storage device can be saved or stored on the device. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, an electronic storage device user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often

maintained indefinitely until overwritten by other data.

44. Based on my knowledge, training, and experience, I know that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

45. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage.

46. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an

individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

47. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who transport, distribute, receive, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

d. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices using forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

e. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Such individuals prefer not to be without their child pornography for any prolonged period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if an individual, uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in the SUBJECT PREMISES, SUBJECT VEHICLE or a device located on ANDERSON, as set forth in Attachment A.

Attachment A

Description of Subject Premises, Subject Vehicle, and Subject Person

1. 2424 W. Wells Street, Milwaukee is a four-story apartment complex. Its exterior is green on the first floor, and brown and tan on the upper floors. There is an awning over the front door which has "2424" on it. There is a driveway and garage door on the first level next to the front door. There are buzzers located adjacent to the front door. There are large windows on the front center of the building showing the stairwell and building hallways. This warrant applies to the apartment designated as "114."

2. white GMC Yukon license plate ALU6909

3. Person of Daniel ANDERSON, date of birth XX/XX/1969

Attachment B

Items To Be Seized

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use, or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252(a)(2)(A), 1591(a)(1)(b)(1), 2251, and 2252(a)(2):

1. Computers or storage media used as a means to commit the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;

b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

d. Records and information relating to the sexual exploitation of children, including correspondence and communications between users of any electronic messaging application;

e. Records and information related to any money transfer or other payment systems; and

f. Records and information showing access to and/or use of any electronic messaging application.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macro-SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the SUBJECT PREMISES, the SUBJECT VEHICLE and the person of ANDERSON, described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of ANDERSON to the Touch ID sensor of the Apple brand device(s), such as an iPhone or iPad or fingerprint scanner or reader of other devices found at the SUBJECT PREMISES or Subject Vehicle for the purpose of attempting to unlock the device via Touch ID/fingerprint scanner or reader in order to search the contents as authorized by this warrant. Law enforcement is also authorized to hold the devices up to ANDERSON's face for facial recognition or iris scanner.

☑ Original ☐

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
ANDERSON's residence, 2424 W. Wells Street, Apt 114, Milwaukee Wisconsin 53233 (SUBJECT PREMISES), ANDERSON's vehicle, a white GMC Yukon license plate ALU6909 (SUBJECT VEHICLE), and ANDERSON's person (DOB XX/XX/1969)

Case No. 24 MJ 11

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

Please see Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

Please see Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 01/22/2024 *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable William E. Duffin.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 01/08/2024 at 10:10 a.m.

William E. Duffin
Judge's signature

City and state: Milwaukee, WI

Honorable William E. Duffin, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

Attachment A

Description of Subject Premises, Subject Vehicle, and Subject Person

1. 2424 W. Wells Street, Milwaukee is a four-story apartment complex. Its exterior is green on the first floor, and brown and tan on the upper floors. There is an awning over the front door which has "2424" on it. There is a driveway and garage door on the first level next to the front door. There are buzzers located adjacent to the front door. There are large windows on the front center of the building showing the stairwell and building hallways. This warrant applies to the apartment designated as "114."

2. white GMC Yukon license plate ALU6909

3. Person of Daniel ANDERSON, date of birth XX/XX/1969

Attachment B

Items To Be Seized

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use, or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252(a)(2)(A), 1591(a)(1)(b)(1), 2251, and 2252(a)(2):

1. Computers or storage media used as a means to commit the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;

b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

d. Records and information relating to the sexual exploitation of children, including correspondence and communications between users of any electronic messaging application;

e. Records and information related to any money transfer or other payment systems; and

f. Records and information showing access to and/or use of any electronic messaging application.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macro-SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the SUBJECT PREMISES, the SUBJECT VEHICLE and the person of ANDERSON, described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of ANDERSON to the Touch ID sensor of the Apple brand device(s), such as an iPhone or iPad or fingerprint scanner or reader of other devices found at the SUBJECT PREMISES or Subject Vehicle for the purpose of attempting to unlock the device via Touch ID/fingerprint scanner or reader in order to search the contents as authorized by this warrant. Law enforcement is also authorized to hold the devices up to ANDERSON's face for facial recognition or iris scanner.